[0013] Still other aspects, features, and advantages of the invention are readily apparent from the following detailed description, simply by illustrating a number of particular embodiments and implementations, including the best mode contemplated for carrying out the invention. The invention is also capable of other and different embodiments, and its several details can be modified in various obvious respects, all without departing from the spirit and scope of the invention. Accordingly, the drawings and description are to be regarded as illustrative in nature, and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The embodiments of the invention are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings:

[0015] FIG. **1** is a diagram of a system capable of processing one or more user inputs to identify at least one potential privacy conflict, thereby causing a collaboration of one or more privacy policies for at least one privacy preserving action, according to one embodiment;

[0016] FIG. **2** is a diagram of the components of the collaboration platform **109**, according to one embodiment;

[0017] FIG. **3** is a flowchart of a process for processing and/or facilitating a processing of the one or more user inputs to identify at least one potential privacy conflict to initiate at least one privacy preserving action, according to one embodiment;

[0018] FIG. **4** is a flowchart of a process for causing a creation of one or more forms for specifying configurable privacy-related data, and determining at least one privacy preserving action based on the one or more determined privacy policies, according to one embodiment;

[0019] FIG. **5** is a flowchart of a process for causing an enforcement of collaborative privacy policies for at least one potential privacy conflict and cause a control of the at least one shared device based on collaborative privacy policies, according to one embodiment;

[0020] FIG. **6** is a flowchart of a process for causing an application of one or more conflict resolution strategies for determining one or more privacy policies based on the negotiation between at least one device and at least one shared device, according to one embodiment;

[0021] FIG. **7** is a flowchart of a process for modification of one or more privacy policies for at least one shared device and a repetition of conflict detection process and/or conflict resolution process based, at least in part, on the modification and/or on determination of an unsatisfactory outcome, according to one embodiment;

[0022] FIG. **8** is a user interface diagram that represents a collaborative privacy policy for a security camera in a residential building, according to one example embodiment;

[0023] FIG. **9** is a user interface diagram that represents a real time architecture involving personal shared device interaction and/or device negotiation, according to one example embodiment;

[0024] FIG. **10** is a diagram of hardware that can be used to implement an embodiment of the invention;

[0025] FIG. **11** is a diagram of a chip set that can be used to implement an embodiment of the invention; and

[0026] FIG. **12** is a diagram of a mobile terminal (e.g., handset) that can be used to implement an embodiment of the invention.

DESCRIPTION OF SOME EMBODIMENTS

[0027] Examples of a method, apparatus, and computer program for processing one or more user inputs to identify at least one potential privacy conflict, thereby causing a collaboration of one or more privacy policies for at least one privacy preserving action are disclosed. In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the embodiments of the invention. It is apparent, however, to one skilled in the art that the embodiments of the invention may be practiced without these specific details or with an equivalent arrangement. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the embodiments of the invention.

[0028] FIG. **1** is a diagram of a system capable of processing one or more user inputs to identify at least one potential privacy conflict, thereby causing a collaboration of one or more privacy policies for at least one privacy preserving action, according to one embodiment. Needless to mention, smart devices are becoming pervasive with different data gathering and sharing needs and capabilities. Specific numbers of such devices are shared, wherein the device is owned by multiple users and the users are responsible for regulating the operation of the shared device. Such shared devices are becoming increasingly popular in home and office building environments, for example, information and communication technologies (ICT) enabled building devices which includes traditional network devices, such as thermostats, sensors, HVAC equipment and lighting fixtures are becoming ubiquitous, leading to a complete landscape of smart devices that can be integrated into a single system. Though such shared devices benefits the users involved, at the same time the privacy of the users are compromised. At the same time, users may have their own preferences and/or restrictions with respect to regulating the usage of the at least one shared device. In one example embodiment, a neighbor's privacy restriction may contradict how the other neighbor wants the security cameras in a residential building to function. The conflict with one's neighbor does not necessarily mean that a security camera cannot be used all, but the neighbor's opposing view needs to be taken into account as this is a shared resource. As a result, a sophisticated approach is required wherein the viewing range for the security camera can be better controlled based, at least in part, on user inputs. Therefore, the objective is to come up with a compromise that best suits the preferences and/or restrictions of the concerned users.

[0029] To address this problem, a system **100** of FIG. **1** introduces the capability to a collaborate one or more privacy policies for at least one shared device to generate at least one privacy preserving action based, at least in part, on one or more identified potential conflict. The one or more potential conflict is identified based, at least in part, on the matching of one or more user inputs. In one embodiment, the system **100** causes an enforcement of one or more collaborative conflict resolving actions for at least one shared device based, at least in part, on privacy policies. The one or more collaborative conflict resolving actions is based, at least in part, on device capabilities, application trustworthiness, or a combination thereof. In another embodiment, the system **100** determines at least one permitted value for one or more configurable privacy-related data of at least one shared device, and causes a selection of at least one permitted value based, at least in part, on privacy policies, user context information, or a combina-